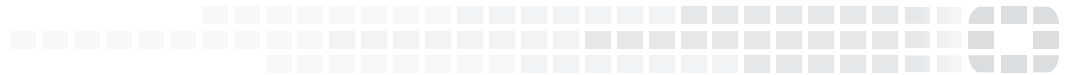




**FORTINET®**  
*High Performance Network Security*



# FortiOS™ Handbook - FortiView

for FortiOS 5.6



**FORTINET DOCUMENT LIBRARY**

<http://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<http://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

<http://cookbook.fortinet.com/how-to-work-with-fortinet-support/>

**FORTIGATE COOKBOOK**

<http://cookbook.fortinet.com>

**FORTINET TRAINING SERVICES**

<http://www.fortinet.com/training>

**FORTIGUARD CENTER**

<http://www.fortiguard.com>

**FORTICAST**

<http://forticast.fortinet.com>

**END USER LICENSE AGREEMENT**

<http://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdocs@fortinet.com](mailto:techdocs@fortinet.com)



September 29, 2017

FortiOS™ Handbook - FortiView

01-561-122872-20170929

# TABLE OF CONTENTS

<b>Change Log</b>	<b>5</b>
<b>Introduction</b>	<b>6</b>
<b>Purpose</b>	<b>7</b>
<b>Overview</b>	<b>8</b>
Enabling FortiView	9
FortiView Feature Support - Platform Matrix	9
Basic feature support	11
Historical Data	12
Disk Logging	13
Configuration Dependencies	13
FortiView interface	15
The FortiView graph	16
Bubble Chart Visualization	16
Links created between FortiView and View/Create Policy	17
Visualization support for the Admin Logins page	17
Realtime visualization	17
Accelerated sessions	17
WHOIS Lookup anchor for public IPv4 addresses	18
<b>FortiView consoles</b>	<b>19</b>
Sources	20
Destinations	21
Applications	22
Cloud Applications	23
Web Sites	24
Threats	25
WiFi Clients	26
Traffic Shaping	27
System Events	28
VPN	29
Endpoint Vulnerability	30
Threat Map	31
Policies	32
Interfaces	33
FortiSandbox	34

All Sessions .....	35
<b>Reference .....</b>	<b>36</b>
Filtering options .....	37
Drill-Down Options .....	40
Columns displayed .....	42
Risk level indicators .....	49
<b>Troubleshooting FortiView .....</b>	<b>50</b>
No logging data is displayed .....	50
Logging is enabled, but data is not appearing .....	50

## Change Log

Date	Change Description
2015-09-01	Official release for FortiOS 5.4.
2016-06-14	Official release for FortiOS 5.4.1.
2017-09-29	Official release for FortiOS 5.6.1.

# Introduction

This document provides a general guide to FortiView, the FortiOS log view tool, explaining its layout, features, and its usefulness in everyday administrative scenarios. This document includes:

- [Overview on page 8](#) outlines the role FortiView plays in FortiOS and its overall layout. This section also identifies which FortiGate platforms support the full FortiView features.
- [FortiView consoles on page 19](#) describes the various FortiView consoles available in FortiOS, including example scenarios, in most cases.
- [Reference on page 36](#) explains reference information for the various consoles in FortiView, and describes the assortment of filtering options, drilldown options, and columns available.
- [Troubleshooting FortiView on page 50](#) offers solutions to common technical issues experienced by FortiGate users regarding FortiView.

## Purpose

FortiView is a comprehensive monitoring system for your network that integrates real-time and historical data into a single view on your FortiGate. It can log and monitor threats to networks, filter data on multiple levels, keep track of administrative activity, and more.

FortiView allows you to use multiple filters within the consoles, enabling you to narrow your view to a specific time (up to 24 hours in the past), by user ID or local IP address, by application, and many more. For more on FortiView's filtering options, see [Filtering options on page 37](#)

FortiView can be used to investigate traffic activity, such as user uploads/downloads or videos watched on YouTube, on a network-wide, user group, and individual-user level, with information relayed in both text and visual format. FortiView makes it easy to get an actionable picture of your network's internet activity.

The degree to which information can be logged will depend on which FortiGate unit you have. For more information, see [Enabling FortiView on page 9](#).

# Overview

This section provides an overview of FortiView, its interface, and options, including the following:

[Enabling FortiView](#)

[FortiView Feature Support - Platform Matrix](#)

[Configuration Dependencies](#)

[FortiView interface](#)



## Enabling FortiView

By default, FortiView is enabled on FortiGates running FortiOS firmware version 5.2 and above. You will find the FortiView consoles in the main menu. However, certain options will not appear unless the FortiGate has **Disk Logging** enabled.

Only certain FortiGate models support Disk Logging. A complete list of FortiGate platforms that support Disk Logging is provided in the matrix below.

### To enable Disk Logging

1. Go to **Log & Report > Log Settings** and select the checkbox next to **Disk**.
2. **Apply** the change.

### To enable Disk Logging - CLI

```
config log disk setting
    set status enable
end
```

## FortiView Feature Support - Platform Matrix

Note that the following table identifies three separate aspects of FortiView in FortiOS 5.2.3:

- [Basic feature support](#)
- [Historical Data](#)
- [Disk Logging](#)

Platform	Basic Feature Support	Disk Logging	Historical Data *
FG/FWF-20C Series	✓		
FG/FWF-30D/40C Series	✓		
FG/FWF-60C Series	✓		
FG/FWF-60D Series	✓		
FGR-60D	✓		
FG-60D	✓		
FG/FWF-80C Series	✓		
FG-80D	✓	✓	1 hour

Platform	Basic Feature Support	Disk Logging	Historical Data *
FG/FWF-90D Series	✓	✓	1 hour
FG/FWF-92D Series	✓		
FG-110C	✓		
FG-111C	✓	CLI	1 hour
FG-100D Series	✓	✓	24 hours
FG-200B Series	✓	#	# (24 hours)
FG-200D Series	✓	✓	24 hours
FG-310B	✓		# (24 hours)
FG-311B	✓		# (24 hours)
FG-300C	✓	✓	24 hours
FG-300D	✓	✓	24 hours
FG-500D	✓	✓	24 hours
FG-620B	✓	#	# (24 hours)
FG-621B	✓	#	# (24 hours)
FG-600C	✓	✓	24 hours
FG-800C	✓	✓	24 hours
FG-1000D	✓	✓	7 hours, 24 hours
FG-1500D	✓	✓	7 hours, 24 hours
FG-1240B	✓	✓	24 hours
FG-3016B	✓	#	# (24 hours)
FG-3040B	✓	CLI	24 hours
FG-3140B	✓	CLI	24 hours
FG-3240C	✓	CLI	24 hours
FG-3600C	✓	CLI	24 hours

Platform	Basic Feature Support	Disk Logging	Historical Data *
FG-3700D/DX	✓	CLI	7 hours, 24 hours
FG-3810A	✓	#	# (24 hours)
FG-3950B	✓	#, CLI	# (24 hours)
FG-3951B	✓	#, CLI	# (24 hours)
FG-5001A	✓	#, CLI	# (24 hours)
FG-5001B	✓	CLI	24 hours
FG-5001C	✓	CLI	24 hours
FG-5001D	✓	CLI	24 hours
FG-5101C	✓	CLI	24 hours
FS-5203B	✓	CLI	

✓ = Default support.

# = Local storage required.

\* Refer to section on Historical Data below.

## Basic feature support

FortiView's consoles give insight into your user's traffic, not merely showing which users are creating the most traffic, but what sort of traffic it is, when the traffic occurs, and what kind of threat the traffic may pose to the network.

FortiView basic feature support consists of the following consoles:

- [Sources](#)
- [Destinations](#)
- [Interfaces](#)
- [Policies](#)
- [All Sessions](#)
- [Applications](#)

The complete array of features in FortiView requires disk logging enabled (see below). It includes those consoles listed above as well as the following:

- [WiFi Clients](#)
- [Cloud Applications](#)
- [Web Sites](#)
- [Threats](#)
- [VPN](#)

## Historical Data

Not all consoles have the same available historical data options, depending on whether or not your traffic is locally stored.

Below is a table showing which features are available for units using local storage, including the historical data options.



Only FortiGate models 100D and above support the 24 hour historical data.

Features	With Local Storage				Without Local Storage			
	Now	5 min	1 hr	24 hr *	Now	5 min	1 hr	24 hr
Sources	✓	✓	✓	✓	✓			
Destinations	✓	✓	✓	✓	✓			
Interfaces	✓	✓	✓	✓				
Policies	✓	✓	✓	✓				
All Sessions	✓	✓	✓	✓	✓			
Applications	✓	✓	✓	✓	✓			
WiFi Clients		✓	✓	✓				
Cloud Applications	✓	✓	✓	✓	✓			
Web Sites	✓	✓	✓	✓				
Threats		✓	✓	✓				
Threat Map	✓				✓			
FortiSandbox		✓	✓	✓				
System Events		✓	✓	✓				
VPN		✓	✓	✓				

\* Not available for desktop models with SSD.

### 7-day time display

As mentioned previously, certain models support 7-day time display. These models are listed below:

- FortiGate 1000D
- FortiGate 1500D
- FortiGate 3700DX
- FortiGate 3700D

The option for 7-day time display, however, can only be configured in the CLI using the following command:

```
config log setting
  set fortiview-weekly-data {enable|disable}
end
```

## Disk Logging

Only certain FortiGate models support Disk Logging (see above).

To enable Disk Logging, go to **Log & Report > Log Settings**, and select the checkbox next to **Disk** and apply the change.

## Configuration Dependencies

Most FortiView consoles require the user to enable several features to produce data. The following table summarizes the dependencies:

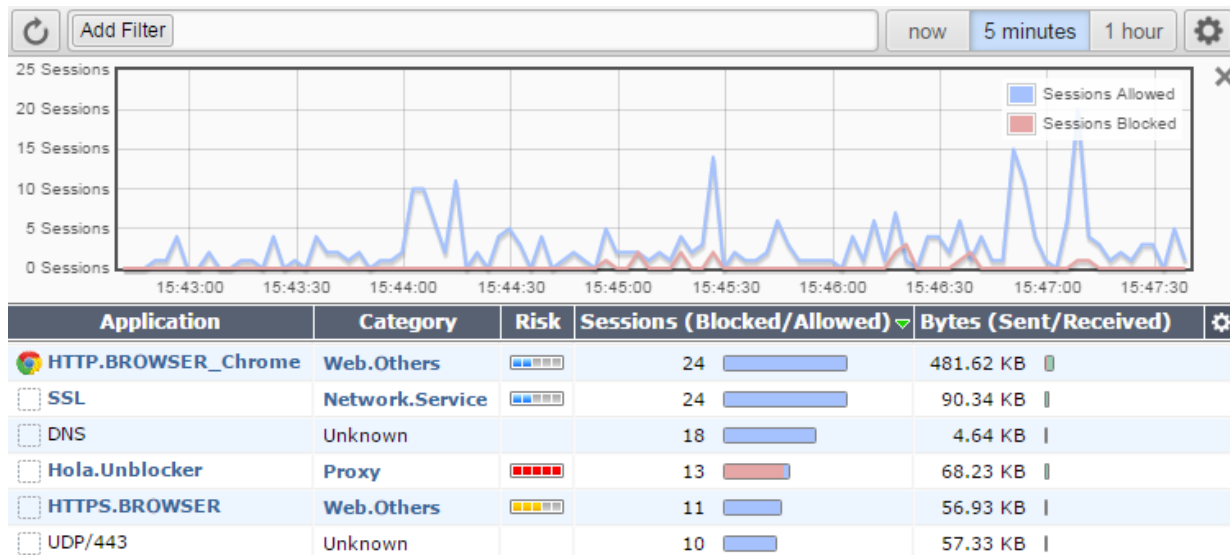
Feature	Dependencies (Realtime)	Dependencies (Historical)
<b>Sources</b>	None, always supported	Traffic logging enabled in policy
<b>Destinations</b>	None, always supported	Traffic logging enabled in policy
<b>Interfaces</b>	None, always supported	Disk logging enabled Traffic logging enabled in policy
<b>Policies</b>	None, always supported	Disk logging enabled Traffic logging enabled in policy
<b>All Sessions</b>	None, always supported	Traffic logging enabled in policy
<b>Applications</b>	None, always supported	Disk logging enabled Traffic logging enabled in policy Application control enabled in policy
<b>WiFi Clients</b>	None, always supported	Disk logging enabled Traffic logging enabled in policy

Feature	Dependencies (Realtime)	Dependencies (Historical)
<b>Cloud Applications</b>	Not supported	Disk logging enabled  Application control enabled in policy  SSL "deep inspection" enabled in policy  Deep application inspection enabled in application sensor  Extended UTM log enabled in application sensor
<b>Web Sites</b>	Disk logging enabled  Web Filter enabled in policy  "web-url-log" option enabled in Web Filter profile	Disk logging enabled  Web Filter enabled in policy  "web-url-log" option enabled in Web Filter profile
<b>Threats</b>	Not supported	Disk logging enabled  Traffic logging enabled in policy  Threat weight detection enabled
<b>Threat Map</b>	None, always supported	Disk logging enabled  Traffic logging enabled in policy  Threat weight detection enabled
<b>FortiSandbox</b>	Not supported	Disk logging enabled  Traffic logging enabled in policy
<b>System Events</b>	Not supported	Disk logging enabled
<b>VPN</b>	Not supported	Disk logging enabled  Traffic logging enabled in policy

## FortiView interface

FortiView lets you access information about the traffic activity on your FortiGate, visually and textually. FortiView is broken up into several consoles, each of which features a top menu bar and a graph window, as seen in the following image:

### FortiView Application console sorted by Sessions (Blocked/Allowed)



The top menu bar features:

- a **Refresh** button, which updates the data displayed,
- a **Filter** button, for filtering the data by category,
- a **Settings** button (containing additional viewing settings and a link to the Threat Weight menu).
- a drop-down menu of different views:
  - **Time Display** (options: now, 5 minutes, 1 hour, or 24 hours),
  - **Table View**
  - **Timeline View**
  - **Bubble Chart**<sup>1</sup>
  - **Country Map**

<sup>1</sup> For information on the Bubble Chart, refer to [Bubble Chart Visualization on page 16](#).



Certain views are only available in specific consoles.

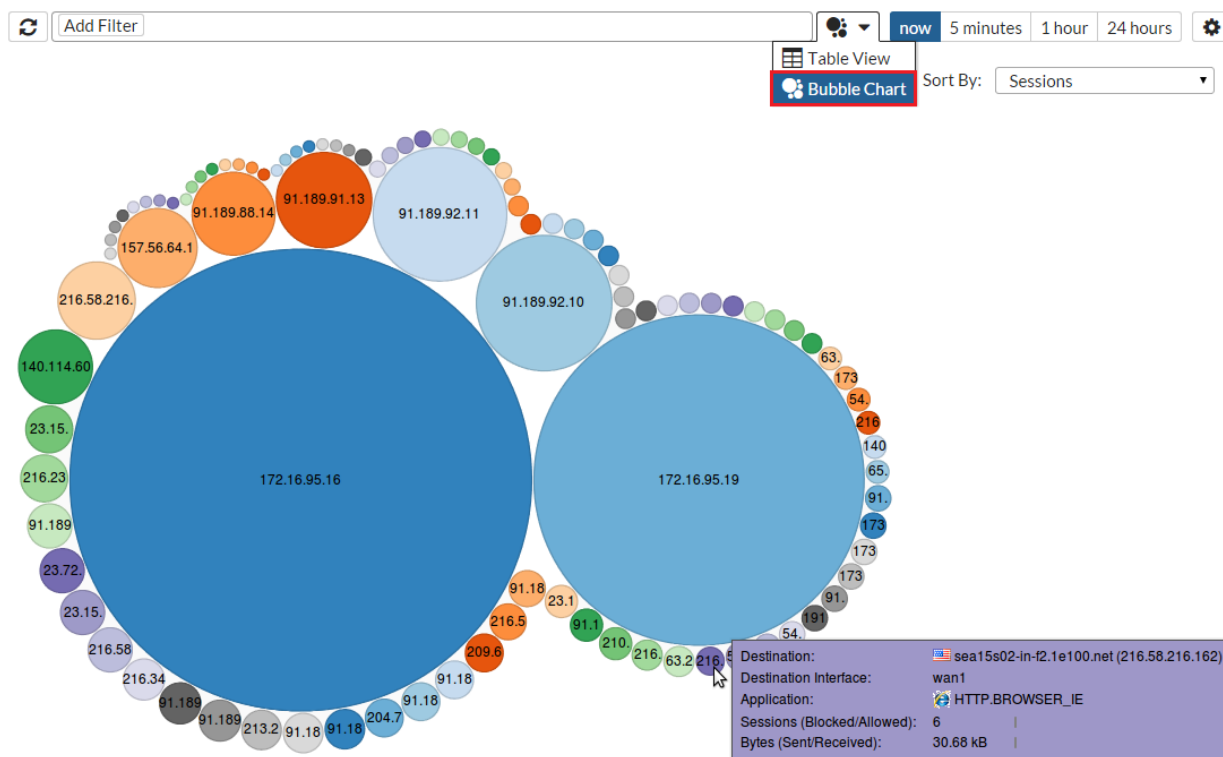
## The FortiView graph

The graph window can be hidden using the **X** in the top right corner, and re-added by selecting **Show Graph**. To zoom in on a particular section of the graph, click and drag from one end of the desired section to the other. This will appear in the **Time Display** options as a **Custom** selection. The minimum selection size is 60 seconds.



Only FortiGate models 100D and above support the 24 hour historical data.

## Bubble Chart Visualization



### Notes about the Bubble Chart:

- It is possible to sort on the Bubble Chart using the **Sort By:** dropdown menu.
- The size of each bubble represents the related amount of data.
- Place your cursor over a bubble to display a tool-tip with detailed info on that item.
- You can click on a bubble to drilldown into greater (filtered) detail.



## Links created between FortiView and View/Create Policy

The **Policy** column in FortiView consoles and the Log Viewer pages includes a link, which navigates to the IPv4 or IPv6 policy list and highlights the policy.

Right-clicking on a row in FortiView or the Log Viewer has menu items for **Block Source**, **Block Destination** and **Quarantine Source** where appropriate columns are available to determine these values. When multiple rows are selected, the user will be prompted to create a named **Address Group** to contain the new addresses.

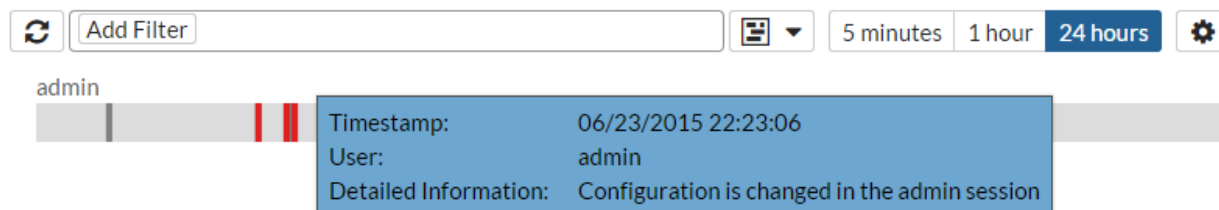
When the user clicks **Block Source** or **Block Destination** they are taken to a policy creation page with enough information filled in to create a policy blocking the requested IP traffic.

The policy page will feature an informational message block at the top describing the actions that will be taken. Once the user submits the form, the requisite addresses, groups and policy will be created at once.

If the user clicks on **Quarantine User** then they will be prompted for a duration. They may also check a box for a **Permanent Ban**. The user can manage quarantined users under **Monitor > Quarantine Monitor**.

## Visualization support for the Admin Logins page

A useful chart is generated for Admin login events under **FortiView > Admin Logins**. You can view the information in either **Table View** or **Timeline View** (shown below). In Timeline View, each line represents on administrator, with individual sessions indicated per administrator line. When you hover over a particular timeline, detailed information appears in a tooltip.



## Realtime visualization

To enable realtime visualization:

1. Click on the **Settings** icon next to the upper right-hand corner and select **Auto update realtime visualizations**. An option is displayed to set the **Interval (seconds)**. The maximum value is 300.
2. Enter a desired **Interval** and click **Apply**.

## Accelerated sessions

When viewing sessions in the [All Sessions](#) console, information pertaining to NP4/ NP6 acceleration is now reflected via an appropriate icon in the table. The tooltip for the icon includes the NP chip type and its total number of accelerated sessions.

### Filtering on accelerated sessions

You can filter the console on 'FortiASIC' ('Accelerated' versus 'Not Accelerated') sessions.

## WHOIS Lookup anchor for public IPv4 addresses

A Reverse IP lookup is possible using the WHOIS lookup icon available when you mouse over a public IP address in a FortiView log. If you left-click on the lookup icon, a new tab is opened in your browser for [www.networksolutions.com](http://www.networksolutions.com), and a lookup is performed on the selected IP address (this option persists after drilling down one level in FortiView).

## FortiView consoles

This section describes the following log filter consoles available in FortiView:

- [Sources on page 20](#) displays detailed information on the sources of traffic passing through the FortiGate, and the section covers how you can investigate an unusual spike in traffic to determine which user is responsible.
- [Destinations on page 21](#) displays detailed information on user destination-accessing through the use of drill down functionality.
- [Applications on page 22](#) displays Applications used on the network that have been recognized by Application Control, and this section shows how you can view what sort of applications individual employees are using.
- [Cloud Applications on page 23](#) displays Web/Cloud Applications used on the network, and this section shows how you can drill down to access detailed data on cloud application usage, e.g. YouTube.
- [Web Sites on page 24](#) displays websites visited as part of network traffic that have been recognized by Web Filtering, and this section shows how you can investigate instances of proxy avoidance, which is the act of circumventing blocks using proxies.
- [Threats on page 25](#) monitors threats to the network, both in terms of their Threat Score and Threat Level.
- [WiFi Clients on page 26](#) displays a list of all the devices connected to the WLAN.
- ["Traffic Shaping" on page 27](#) displays a list of existing Traffic Shapers, detailing their bandwidth use and which traffic is being shaped by each shaper.
- [System Events on page 28](#) displays security events detected by FortiOS, providing a name and description for the events, an assessment of the event's severity level, and the number of instances the events were detected.
- [VPN on page 29](#) displays how users can access information on any VPNs associated with their FortiGate.
- ["Endpoint Vulnerability" on page 30](#) displays a list of Vulnerability events detected by the FortiGate on networked devices, along with links to further vulnerability information and databases.
- [Threat Map on page 31](#) provides a geographical display of threats, in realtime, from international sources as they arrive at your FortiGate.
- [Policies on page 32](#) displays what policies are in affect on your network, what their source and destination interfaces are, how many sessions are in each policy, and what sort of traffic is occurring.
- [Interfaces on page 33](#) displays the number of interfaces connected to your network, how many sessions there are in each interface, and what sort of traffic is occurring.
- [FortiSandbox on page 34](#) displays FortiSandbox activity. FortiSandbox detects and analyzes advanced attacks designed to bypass traditional security defenses, and has a wide array of features that allow it to prevent future attacks from occurring again.
- [All Sessions on page 35](#) displays complete information on all FortiGate sessions, with the ability to filter sessions by port number and application type.

## Sources

The **Sources** console provides information about the sources of traffic on your FortiGate unit.

This console can be filtered by Country, Destination Interface, Policy, Result, Source, and Source Interface. For more on filters, see [Filtering options](#).

Specific devices and time periods can be selected and drilled down for deep inspection.

### Scenario: Investigating a spike in traffic

A system administrator notices a spike in traffic and wants to investigate it. From the **Sources** window, they can determine which user is responsible for the spike by following these steps:

1. Go to **FortiView > Sources**.
2. In the graph display, click and drag across the peak that represents the spike in traffic.
3. Sort the sources by bandwidth use by selecting the **Bytes (Sent/Received)** header.
4. Drill down into whichever source is associated with the highest amount of bandwidth use by double-clicking it. From this screen, you have an overview of that source's traffic activity.
5. Again, in either the **Applications** or **Destinations** view, select the **Bytes (Sent/Received)** header to sort by bandwidth use.
6. Double-click the top entry to drill down to the final inspection level, from which you can access further details on the application or destination, and/or apply a filter to prohibit or limit access.



Only FortiGate models 100D and above support the 24 hour historical data.

---

## Destinations

The **Destinations** console provides information about the destination IP addresses of traffic on your FortiGate unit, as well as the application used. You can drill down the displayed information, and also select the device and time period, and apply search filters.

This console can be filtered by Country, Destination Interface, Destination IP, Policy, Result, and Source Interface. For more on filters, see [Filtering options](#).

### Scenario: Monitoring destination data

The Destinations console can be used to access detailed information on user destination-accessing through the use of the console's drilldown functionality. In this scenario, the console is used to find out more about a particular user's Facebook usage patterns over a 24-hour period:

1. Go to **FortiView > Destinations**.
2. Select **1 hour** from the Time Display options at the top right corner of the console.
3. The easiest way to locate most destinations is to scan the Applications column for the name of the application. Once the session containing Facebook has been located, double-click it to access the Destination summary window.
4. Locate Facebook in the Applications column and double-click it to view the Facebook drilldown page. From here, detailed information regarding the user's Facebook session can be accessed.



Only FortiGate models 100D and above support the 24 hour historical data.

---

## Applications

The **Applications** console provides information about the applications being used on your network.

This console can be filtered by Application, Country, Destination Interface, Policy, Result, and Source Interface. For more on filters, see [Filtering options](#).

Specific devices and time periods can be selected and drilled down for deep inspection.



In order for information to appear in the **Applications** console, Application Control must be enabled in a policy.

---

### Scenario: Viewing application usage

A manager is interested in the office internet habits of their employees:

1. Go to **FortiView > Applications**, to view the list of applications accessed by the users on your network. Use the time-frame options to view what applications were used in those time periods (from now, 5 minutes, 1 hour, or 24 hours).
2. From **Sessions (Blocked/Allowed)** and **Bytes (Sent/Received)**, you can see how much traffic has been generated. Click these columns to show the traffic in descending order.
3. You notice that a social media application has created the most traffic of all the applications, and so it's at the top of the list. Drill down into the application by double-clicking or right-clicking and select **Drill Down to Details**.
4. You are directed to a summary page of the social media application. From here, you can see which specific user has made the most use of the application.



Only FortiGate models 100D and above support the 24 hour historical data.

---

## Cloud Applications

The **Cloud Applications** console provides information about the cloud applications being used on your network. This includes information such as:

- The names of videos viewed on YouTube (visible by hovering the cursor over the session entry)
- Files uploaded and downloaded from cloud hosting services such as Dropbox
- Account names used for cloud services

Two different views are available for the Cloud Applications: **Applications** and **Users** (located in the top menu bar next to the time periods). **Applications** shows a list of the programs being used. **Users** shows information on the individual users of the cloud applications, including the username, if the FortiGate was able to view the login event.

This console can be filtered by Cloud Application and Result. For more on filters, see [Filtering options](#).



In order for information to appear in the **Cloud Applications** console, an application control profile (that has Deep Inspection of Cloud Applications turned on) must be enabled in a policy, and SSL Inspection must use `deep-inspection`.

### Scenario: Viewing cloud application usage data

From the Cloud Applications console, users can drill down to access detailed data on cloud application usage data. In this scenario, the console is used to determine the network's most frequent user of YouTube over a 24-hour period, and find out more about their usage patterns.

1. Go to **FortiView > Cloud Applications**.
2. Select **Applications** view from the top menu bar if it is not already selected.
3. Select **24 Hours** from the Time Display options.
4. Find **YouTube** under the Application column and double-click it (or right-click and select **Drill down for details...**). This will open the YouTube stats window.
5. To determine the user who has accessed YouTube the most frequently, sort the column entries by **Sessions** by selecting the column header of the same name.
6. Double-click (or right-click and select **Drill down for details...**) the top-bandwidth YouTube user to view detailed stats, including the names of videos watched by the user and the date and time each video was accessed.



Only FortiGate models 100D and above support the 24 hour historical data.

## Web Sites

The **Web Sites** console lists the top allowed and top blocked web sites. You can view information by domain or by FortiGuard categories by using the options in the top right corner. Each FortiGuard category can be selected in order to see a description of the category and several example sites, with content loaded from FortiGuard on demand.

This console can be filtered by Domain and Result. For more on filters, see [Filtering options](#).



In order for information to appear in the **Web Sites** console, web filtering must be enabled in a policy, with FortiGate Categories enabled.

---

### Scenario: Investigating an instance of Proxy Avoidance

In this scenario, the Categories view will be used to investigate an instance of Proxy Avoidance, one of the Categories recognized by FortiOS. Proxy Avoidance denotes the use of a proxy site in order to access data that might otherwise be blocked by the server.

1. Go to **FortiView > Web Sites** to open the Web Sites console.
2. Select **Categories** from the top bar menu to enter Categories view.
3. Scan the **Categories** column and locate the instance of Proxy Avoidance, then double-click it to enter its drilldown screen.



Only FortiGate models 100D and above support the 24 hour historical data.

---



## Threats

The **Threats** console lists the top users involved in incidents, as well as information on the top threats to your network.

The following incidents are considered threats:

- Risk applications detected by application control
- Intrusion incidents detected by IPS
- Malicious web sites detected by web filtering
- Malware/botnets detected by antivirus

This console can be filtered by Country, Destination Interface, Policy, Result, Security Action, Source Interface, Threat, and Threat Type. For more on filters, see [Filtering options](#).



In order for information to appear in the **Threats** console, Threat Weight Tracking must be enabled.

---

### Scenario: Monitoring Threats to the Network

Some users have high Threat Scores. The Threats console can be used to view all threats and discover why such high scores are being shown:

1. Go to **FortiView > Threats**. In the graph display, click and drag across the peak that represents the spike in threat score.
2. Sort the threats by score or level by selecting the **Threat Score (Blocked/Allowed)** or the **Threat Level** headers respectively.
3. You see that a specific threat's Threat Level is at Critical. Drill down into the threat by double-clicking or right-clicking and select **Drill down to details**.
4. From this summary page, you can view the source IPs and the number of sessions that came from this threat. Double-click on one of them.
5. The following page shows a variety of statistics, including **Reference**. The URL next to it will link you to a FortiGuard page where it will display the description, affected products, and recommended actions, if you are not familiar with the particular threat.



Only FortiGate models 100D and above support the 24 hour historical data.

---

## WiFi Clients

The **WiFi Clients** console shows a list of all the devices connected to the WLAN. The type of device, source, number of sources blocked and allowed, and bytes sent and received are displayed. The source's Service Set Identifier (SSID) is also displayed in the **Source SSID** column. An SSID is a case sensitive, 32 character alphanumeric identifier that acts as a password when a mobile device tries to connect to the WLAN.

This console can be filtered by AP, Device Type, Result, Source Device, Source IP, Source SSID, and User. For more on filters, see [Filtering options](#).

### Scenario: Determining the threat risk of an individual WiFi client

In this scenario, the administrator will use the WiFi Clients FortiView console to determine the risk levels associated with an individual WiFi client, and then drilldown into that client to determine where the risk originates and who might be the offending user/IP.

1. Go to **FortiView > WiFi Clients** and view the device list table.
2. Double-click on a device to filter on that source.
3. Under the **Risk** column, identify the items that present the greatest risk (using the **Applications**, **Destinations**, **Threats**, and/or **Sessions** tabs, for example).
4. Right-click these items for further action.

## Traffic Shaping

The **Traffic Shaping** console provides information about FortiGate Traffic Shapers that are currently in effect. This console can be filtered by Traffic Shaper Name. For more on filters, see [Filtering options](#).

A number of columns available in FortiView are only available in Traffic Shaping. For example, the **Shaper** column displays the name of the Shaper, which can be used to monitor the traffic being shaped by Bytes Sent, Received, and Dropped, so that bandwidth patterns and Shaper effectiveness can be analyzed.



Only FortiGate models 100D and above support the 24 hour historical data.

---

## System Events

The **System Events** console lists security events detected by FortiOS, providing a name and description for the events, an assessment of the event's severity level (**Alert**, **Critical**, **Emergency**, **Error**, or **Warning**), and the number of instances the events were detected.

Two other FortiView pages from 5.4 have been wrapped into the **System Events** page as of 5.6: **Admin Logins**, and **Failed Authentication**.

This console can be filtered by Event Name, Result, and Severity. For more on filters, see [Filtering options on page 37](#).

### Scenario: Investigate network security events

System Events can be used in conjunction with All Sessions to see what network security events took place, and specifically see what action was taken upon their detection:

1. Go to **FortiView > System Events** to see what and how many network events have taken place, as well as how severe they are in terms of the threat they pose to the network.
2. You see that a particular event has warranted a severe rating, and has allowed traffic to bypass the firewall. Note when the event took place, and go to **FortiView > All Sessions**, to see more information pertaining to the security event.
3. From this console, you can determine the system event's source, how much traffic was sent and received, and the security action taken in response to this security event. These actions differ, depending upon the severity of the security event. See the entry for **Security Action** in [Columns displayed on page 42](#).



Only FortiGate models 100D and above support the 24 hour historical data.

---

## VPN

From the **VPN** console, users can access information on any VPNs associated with their FortiGate. From the initial window, a list of all the associated VPNs is provided, along with general information, such as number of user connections and VPN type. By double-clicking on an individual VPN (or right-clicking and selecting **Drill down for details...**), users can access more specific data on that VPN.

Logs in the VPN console can be sorted by number of connections, last connection time, or data sent/received by selecting the column headers.

This console can be filtered by Result, User Name, and VPN Type. For more on filters, see [Filtering options on page 37](#).



Certain dashboard options will not appear unless your FortiGate has Disk Logging enabled.

Furthermore, only certain FortiGate models support Disk Logging — refer to the [FortiView Feature Support - Platform Matrix on page 9](#) for more information.

To enable Disk Logging, go to **Log & Report > Log Settings**, and select the checkbox next to **Disk** and apply the change.

### Scenario: Investigating VPN user activity

The VPN console can be used to access detailed data on VPN-user activity via the use of the drill down windows. In this scenario, the administrator looks into the usage patterns of the IPsec user who has most frequently connected to the network.

1. Go to **FortiView > VPN** to view the VPN console.
2. Select the **Connections** column header to sort the entries by number of connections to the network.
3. Locate the top user whose VPN Type is **ipsec** and double-click the entry to enter that user's drill down screen.
4. To get the most representative data possible, sort the entries by bandwidth use by selecting the **Bytes (Sent/Received)** column header. Double-click the top entry to enter the drill down window for that connection instance.

From this screen, the administrator can find out more about the specific session, including the date/time of access, the XAuth (Extensible Authentication) User ID, the session's Tunnel ID, and more.



Only FortiGate models 100D and above support the 24 hour historical data.

## Endpoint Vulnerability

The **Endpoint Vulnerability** console lists the top devices and vulnerabilities detected, organized either by frequency or risk level.

This console can be filtered by Vulnerability Name, Severity, Vulnerability Category, CVE-ID, or Host Count. For more on filters, see [Filtering options](#).

The Vulnerabilities detected by the FortiGate use definitions created by FortiGuard, and every vulnerability in FortiView contains a link to the respective FortiGuard Labs documentation page (under the '**Vulnerability ID**' column) and the Common Vulnerabilities and Exposures documentation page (under the '**CVE-ID**' column.)

### Scenario: Monitoring Vulnerabilities on the Network

When a vulnerability appears in log data, you can use the FortiView page to see more information about it. The Endpoint Vulnerability console can be used to view and track all historical vulnerabilities:

1. Go to **FortiView > Endpoint Vulnerability**. In the upper right, select **Vulnerability**.
2. Sort the threats by frequency by selecting the **Host Count** header.
3. You see that a frequent vulnerability's Severity is at Critical. Drill down into the threat by double-clicking or right-clicking and select **Drill down to details**.
4. From this summary page, you can view the source IPs and devices on which this vulnerability was detected, and also the **Scan Time**. Double-click on one of them.
5. The chart will be filtered to display the specific Endpoint and Vulnerability, offering more granular data about the vulnerability, including its Category and the FortiClient ID of the device. You can access the CVE and FortiGuard links from this page to learn more.



Only FortiGate models 100D and above support the 24 hour historical data.

---

## Threat Map

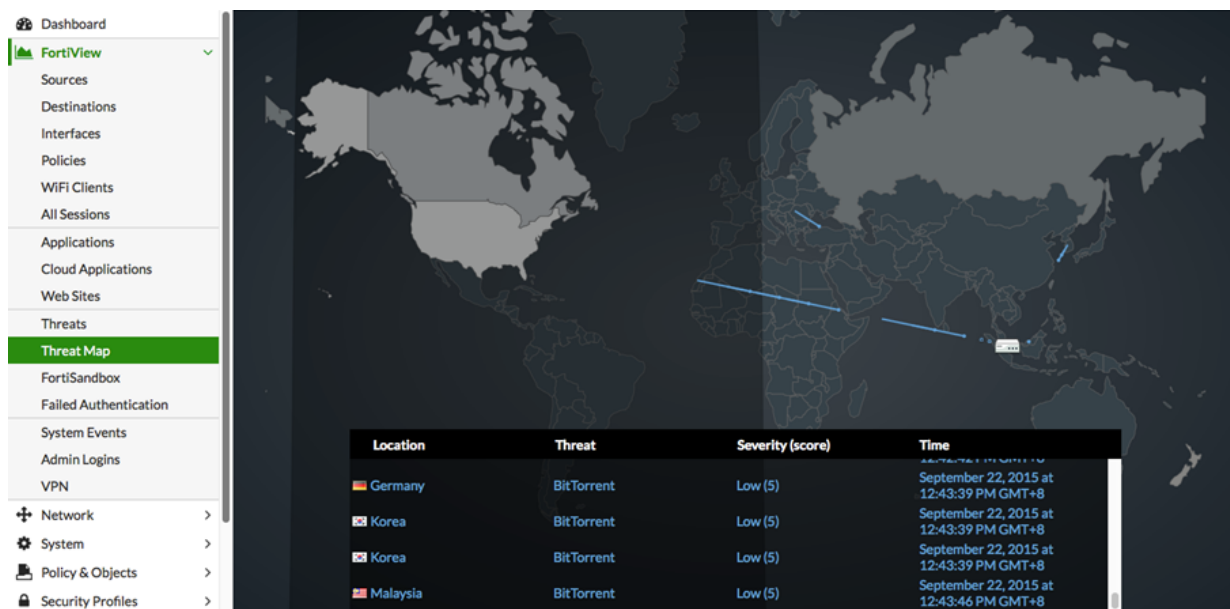
The **Threat Map** console displays network activity by geographic region. Threats from various international destinations will be shown, but only those arriving at your destination, as depicted by the FortiGate. You can place your cursor over the FortiGate's location to display the device name, IP address, and the city name/location.

A visual lists of threats is shown at the bottom, displaying the location, severity, and nature of the attacks. The color gradient of the darts on the map indicate the traffic risk, where red indicates the more critical risk.

Unlike other FortiView consoles, this console has no filtering options, however you can click on any country to drill down into greater (filtered) detail.



Only FortiGate models 100D and above support the 24 hour historical data.



### Scenario: Investigate various international threats

The Threat Map console can be used to regionalize areas that you are more interested in, and disregard regions that you are not interested in:

1. Go to **FortiView > Threat Map** to see a real-time map of the globe. This will show various incoming threats from multiple destinations around the world, depending upon where the FortiGate is placed on the map.
2. You are not interested with threats that are being sent to Eastern Europe, however you are concerned with threats that may be sent to a city in North America. Click and drag the FortiGate to the approximate location where you would like to monitor the incoming threats.
3. To see which countries are sending the more severe threats to your region/location, either see where the red darts are coming from, or check the visual lists of threats at the bottom.

## Policies

The **Policies** console shows what policies are in affect on your network, what their source and destination interfaces are, how many sessions are in each policy, and what sort of traffic is occurring, represented in bytes sent and received.

This console can be filtered by Country, Destination Interface, Destination IP, Policy, Source, Source Device, and Source Interface. For more on filters, see [Filtering options](#).

---



Only FortiGate models 100D and above support the 24 hour historical data.

---

### Scenario: Investigate which policies are in effect

You can click on policy IDs to drill down to the policy list and see what policy's are in effect for specific interfaces, how many sessions have occurred, how many of those with the policy have been blocked, and more:

1. Go to **FortiView > Policies**, and double-click on a policy ID to drill down.
2. You will be redirected to a summary screen of the policy ID. From here you can view the source IP of where the policy has been used, what source interface has been using the particular policy, and to verify what sort of threat scores have been measured, both blocked and allowed.



## Interfaces

The **Interfaces** console lists the total number of interfaces connected to your network, how many sessions there are in each interface, and what sort of traffic is occurring, represented in both bytes sent and received, and the total bandwidth used.

This console can be filtered by Country, Destination Interface, Destination IP, Policy, Result, Source, and Source Interface. For more on filters, see [Filtering options](#).



Only FortiGate models 100D and above support the 24 hour historical data.

---

### Scenario: Investigate traffic spikes per user

The wan1 interface is showing a higher amount of traffic than usual. A system administrator uses the console to inspect which user (as represented by an IP address) is creating the spike in traffic:

1. Go to **FortiView > Interfaces** and double-click on wan1, or right click and select **Drill Down to Details....**
2. The console will drill down to a summary page of wan1, showing how many bytes are being sent and received, how much bandwidth is being used, and how many sessions are currently using this interface. You see the IP address of the user that is showing the most amount of traffic under **Source**.
3. You can further drill down to see the IP destination, the device, and the applications being used, and other options.

## FortiSandbox

The **FortiSandbox** console detects and analyzes advanced attacks designed to bypass traditional security defenses, and has a wide array of features that allow it to prevent future attacks from occurring again.

This console can be filtered by Checksum, File Name, Source, Status, and User Name. For more on filters, see [Filtering options](#).

---



Only FortiGate models 100D and above support the 24 hour historical data.

---

## All Sessions

The **All Sessions** console provides information about all FortiGate traffic. This console can be filtered by Application, Country, Destination Interface, Destination IP, Destination Port, NAT Source IP, NAT Source Port, Policy, Protocol, Source, Source Interface, Source IP, and Source Port. For more on filters, see [Filtering options](#).

This console has the greatest number of column options to choose from. To choose which columns you wish to view, select the column settings cog at the far right of the columns and select your desired columns. They can then be clicked and dragged in the order that you wish them to appear.

A number of columns available in FortiView are only available in All Sessions. For example, the **Action** column displays the type of response taken to a security event. This function can be used to review what sort of threats were detected, whether the connection was reset due to the detection of a possible threat, and so on. This would be useful to display alongside other columns such as the **Source**, **Destination**, and **Bytes (Sent/Received)** columns, as patterns or inconsistencies can be analyzed.

Similarly, there are a number of filters that are only available in All Sessions, one of which is **Protocol**. This allows you to display the protocol type associated with the selected session, e.g. TCP, FTP, HTTP, HTTPS, and so on.

### Scenario: Filtering sessions by port number and application type

From the **All Sessions** console, a wide variety of filters can be applied to sort the session data. In this example, the All Sessions filters will be used to locate a specific user's recent Skype activity.

1. Go to **FortiView > All Sessions**.
2. Select **now** from the **Time Display** options if it is not already selected.
3. Select the **Filter** button, then select **Applications**. This will open a drop-down menu listing the applications that appear in the master session list. From this list, locate and select **Skype**, or type "Skype" into the Search Bar and hit **Enter**. This will filter the session list to only feature Skype usage.
4. Select the **Filter** button again, then select **Destination Port** from the drop-down menu, then locate and select the desired port number. This will add a second filter which will restrict the results to presenting only the Skype data associated with that port number.



Only FortiGate models 100D and above support the 24 hour historical data.

---

## Reference

This section consists of reference information for the various consoles in FortiView. Each console has an assortment of filtering options, drilldown options, and columns that can be displayed. Since many of these options and columns persist through each console, the entire list of options and their descriptions is included below. Attempts have been made to identify the instances where an option or column is only available to a particular console.

This section includes:

[Filtering options](#)

[Drill-Down Options](#)

[Columns displayed](#)

[Risk level indicators](#)

## Filtering options

When you select the **Add Filter** button, a drop-down list appears with a list of available filtering options. Available options differ based on which console is currently being viewed. The following table explains all of the available filtering options:

Filter option	Description
<b>Accelerated Sessions</b>	You can filter the console on 'FortiASIC' ('Accelerated' versus 'Not Accelerated') sessions.
<b>AP</b>	Filter by Access Point (AP) identification number.
<b>Application</b>	Filter by application name.
<b>Checksum</b>	Filter by checksum value. Checksums are reference digits used to represent the correct datatum of a packet in order to detect errors.
<b>Cloud Application</b>	Filter by cloud application name.  <b>Note:</b> This filter is only available in the <b>Cloud Applications</b> console.
<b>Country</b>	Filter by the country from which the source accessed the server.
<b>Destination Interface</b>	Filter by the interface type used by the destination user, e.g. wan1.
<b>Destination IP</b>	Filter by the IP address used by the destination.
<b>Destination Port</b>	Filter by the port used by the destination.  <b>Note:</b> This filter is only available in the <b>All Sessions</b> console, (viewing the <b>now</b> time display).
<b>Domain</b>	Filter by domain name.  <b>Note:</b> This filter is only available in the <b>Web Sites</b> console.
<b>Event Name</b>	Filter by security event name.  <b>Note:</b> This filter is only available in the <b>System Events</b> console.
<b>File Name</b>	Filter by file name.  <b>Note:</b> This filter is only available in the <b>FortiSandbox</b> console.

Filter option	Description
<b>Login Type</b>	Filter by type of login (eg. WEP) associated with the displayed authentication attempt.  <b>Note:</b> This filter is only available in the <b>Failed Authentications</b> console.
<b>NAT Source IP</b>	Filter by the NAT-translated source IP address.  <b>Note:</b> This filter is only available in the <b>All Sessions</b> console, (viewing the <b>now</b> time display).
<b>NAT Source Port</b>	Filter by the NAT-translated source interface.  <b>Note:</b> This filter is only available in the <b>All Sessions</b> console, (viewing the <b>now</b> time display).
<b>Policy</b>	Filter by the policy identification number.
<b>Protocol</b>	Filter by the protocol used by the source, e.g. tcp or udp.  <b>Note:</b> This filter is only available in the <b>All Sessions</b> console, (viewing the <b>now</b> time display).
<b>Result</b>	Filter by the result of whatever security action was taken by FortiOs in the selected session, eg. Accept (all).
<b>Security Action</b>	Filter by the type of response taken to the security event. The types of possible actions are as follows:  <b>Allowed:</b> No threat was detected and the connection was let through.  <b>Blocked:</b> A threat was detected and the connection was not let through.  <b>Reset:</b> A possible issue was detected and the connection was reset.  <b>Traffic Shape:</b> Some data packets may have been delayed to improve system-wide performance.
<b>Severity</b>	Filter by the severity level ( <b>Critical</b> , <b>High</b> , <b>Medium</b> or <b>Low</b> ) associated with a security event.
<b>Source</b>	Filter by the source IP address.
<b>Source IP</b>	
<b>Source Device</b>	Filter by source device type, e.g. mobile.
<b>Source Interface</b>	Filter by the interface type used by the source user, e.g. wan1.

Filter option	Description
Source Port	Filter by the source interface.  <b>Note:</b> This filter is only available in the <b>All Sessions</b> console,(viewing the <b>now</b> time display).
Source SSID	Filter by the Service Set Identifier (SSID) associated with the selected user. An SSID is a case sensitive, 32 character alphanumeric identifier that acts as a password attributed to a mobile device.
Status	Filter by the maliciousness of a file. The types of possible status' are <b>Malicious, High, Medium, Low, Clean, Unknown, and Pending</b> .  <b>Note:</b> This filter is only available in the <b>FortiSandbox</b> console.
Threat	Filter by threat name and/or URL
Threat Type	Filter by threat category, e.g. <i>Illegal/Unethical</i> or <i>P2P</i> .
Type	<b>Note:</b> This filter is only available in the <b>Failed Authentications</b> console.
User Name	Filter by user name.
VPN Type	Filter by Virtual Private Network (VPN) protocol type, eg. <i>PPTP</i> .  <b>Note:</b> This filter is only available in the <b>VPN</b> console.

## Drill-Down Options

Double-click, or right-click, on any entry in a FortiView console and select **Drill Down to Details**, to view the following columns (options vary depending on the console selected):



Drill down options are available for all FortiView consoles except **All Sessions**, **Logical Topology**, and **Physical Topology**.

Option	Description
<b>Applications</b>	Select to drill down by application to view application-related information, including the application name, sessions blocked and allowed, bytes sent and received, and the risk level. You can sort entries by selecting the column header.
<b>Sources</b>	Select to drill down by rows to view source-related information, including IP address, device type, interface type, threat score, number of sessions blocked/allowed, and bytes sent/received. You can sort entries by selecting the column header.
<b>Destinations</b>	Select to drill down by destination to view destination-related information, including the IP address and geographic region, interface, threat score, number of sessions blocked and allowed, and bytes sent and received. You can sort entries by selecting the column header.
<b>Countries</b>	Select to drill down by country, including the number of sessions, bytes sent and received, and the bandwidth used. You can sort entries by selecting the column header.
<b>Policies</b>	Select to drill down by the policies in use, including source interface, destination interface, bytes sent and received, and bandwidth used. You can sort entries by selecting the column header.
<b>Source Interfaces</b>	Select to drill down by source interface, including bytes sent and received, and bandwidth used. You can sort entries by selecting the column header.
<b>Destination Interfaces</b>	Select to drill down by destination interface, including bytes sent and received, and bandwidth used. You can sort entries by selecting the column header.
<b>Threats</b>	Select to drill down by threat to view threat-related information, including the threat name, category, threat level, threat score, and number of sessions blocked and allowed. You can sort entries by selecting the column header.
<b>Domains</b>	Select to drill down by domain to view domain-related information, including domain name, category, browsing time, threat weight, number of sessions blocked/allowed, and bytes sent/received. You can sort entries by selecting the column header.



Option	Description
<b>Categories</b>	Select to drill down by category to view category-related information, including category name, browsing time, threat score, number of sessions blocked/allowed, and bytes sent/received. You can sort entries by selecting the column header.
<b>Sessions</b>	Select to drill down by sessions to view session-related information, including date/time, source, destination IP address and geographic region, application name, security action, security event, and bytes sent/received. You can sort entries by selecting the column header.

## Columns displayed

The following columns appear in the initial window of the dashboards. Some columns may only be visible by selecting them from the column drop-down menu. Options vary depending on the dashboard selected.

Column name	Description
<b>Action</b>	<p>Displays the type of response taken to a security event. The types of possible actions are as follows:</p> <ul style="list-style-type: none"><li>• <b>Allowed:</b> No threat was detected and the connection was let through.</li><li>• <b>Blocked:</b> A threat was detected and the connection was not let through.</li><li>• <b>Reset:</b> A possible issue was detected and the connection was reset.</li><li>• <b>Traffic Shape:</b> Some data packets may have been delayed to improve system-wide performance.</li></ul> <p><b>Note:</b> This column is only available in the <b>All Sessions</b> console.</p>
<b>Application</b>	<p>Displays the application name and service. When <b>Time Display</b> is set to <b>now</b>, you can access further information about an application by selecting the column entry.</p>
<b>Application Category</b>	<p>Displays the type of application used in the selected session, e.g. video player, social media.</p> <p><b>Note:</b> This column is only available in the <b>All Sessions</b> console.</p>
<b>Application ID</b>	<p>Displays the identification number associated with the application used in the selected session.</p> <p><b>Note:</b> This column is only available in the <b>All Sessions</b> console.</p>

Column name	Description
<b>Application Risk</b> <b>Risk</b>	<p>Displays the application risk level. You can hover the mouse cursor over the entry in the column for additional information, and select the column header to sort entries by level of risk.</p> <p>Risk uses a 5-point risk rating. The rating system is as follows:</p> <ul style="list-style-type: none"> <li>• <b>Critical:</b> Applications that are used to conceal activity to evade detection.</li> <li>• <b>High:</b> Applications that can cause data leakage, are prone to vulnerabilities, or may download malware.</li> <li>• <b>Medium:</b> Applications that can be misused.</li> <li>• <b>Elevated:</b> Applications that are used for personal communications or can lower productivity.</li> <li>• <b>Low:</b> Business-related applications or other harmless applications.</li> </ul>
<b>Bandwidth</b>	Displays information for bandwidth calculated on a per-session level, providing administrators the ability to sort realtime bandwidth usage in descending order.
<b>Browsing Time</b>	<p>Displays the amount of time a user has spent browsing a web site (in seconds).</p> <p><b>Note:</b> This column is only available in the <b>Web Sites</b> console, in <b>Categories</b> view..</p>
<b>Bytes</b> <b>(Sent/Received)</b>	<p>Displays the size of sent and received data packets, as measured in bytes. Select the column header to sort the entries by size.</p> <p><b>Note:</b> This information is available on some consoles as two separate columns: <b>Sent</b> and <b>Received</b>.</p>
<b>Category</b>	Displays the category descriptor appropriate to whatever console is being displayed. For example, threat categories are displayed in the Threats console.
<b>Cloud User</b>	<p>Displays the users accessing cloud applications by IP address.</p> <p><b>Note:</b> This column is only available in the <b>Cloud Applications</b> console, in <b>Users</b> view.</p>
<b>Configuration Changes</b>	<p>Displays the number of configuration changes made by the user. You can hover the mouse cursor over an entry for additional information.</p> <p><b>Note:</b> This column is only available in the <b>Admin Logins</b> console.</p>

Column name	Description
<b>Connections</b>	Displays the number of VPN connections made by the selected user..  <b>Note:</b> This column is only available in the <b>VPN</b> console.
<b>Country</b>	Displays the country from which the selected traffic is originating.  <b>Note:</b> This column is only available in the <b>Countries</b> console.
<b>Destination</b>	Displays the destination name, IP address and geographic region.
<b>Destination Country</b>	Displays the country session data is being sent to.  <b>Note:</b> This column is only available in the <b>All Sessions</b> console.
<b>Destination Interface</b>	Displays which interface session data is being sent through, e.g. wan1.
<b>Destination Port</b>	Displays the port number of the destination server being used to accept data.  <b>Note:</b> This column is only available in the <b>All Sessions</b> console.
<b>Device</b>	Displays the device IP address or Fully Qualified Domain Name (FQDN).
<b>Domain</b>	Displays the domain associated with the selected web site, e.g. google.com.  <b>Note:</b> This column is only available in the <b>Web Sites</b> console.
<b>DST Nat IP</b> <b>NAT Destination</b>	Displays the Network Address Translation (NAT) IP address associated with the destination server.  <b>Note:</b> This column is only available in the <b>All Sessions</b> console.
<b>DST Nat Port</b> <b>NAT Destination Port</b>	Displays the Network Address Translation (NAT) port number associated with the destination server.  <b>Note:</b> This column is only available in the <b>All Sessions</b> console.
<b>Duration</b>	Displays the amount of time (in seconds) a user has been logged in.  <b>Note:</b> This column is only available in the <b>Admin Logins</b> console.
<b>Event Name (Description)</b>	Displays the name and description of the selected security event.  <b>Note:</b> This column is only available in the <b>System Events</b> console.

Column name	Description
<b>Events</b>	<p>Displays the number of security events that occurred within a selected session.</p> <p><b>Note:</b> This column is only available in the <b>System Events</b> console.</p>
<b>Expires</b>	<p>Displays the amount of time a session has (in seconds) before it is set to expire.</p> <p><b>Note:</b> This column is only available in the <b>All Sessions</b> console, in <b>now</b> Time Display view.</p>
<b>Failed Logins</b>	<p>Displays the number of failed login attempts made by an administrator over the specified time period.</p> <p><b>Note:</b> This column is only available in the <b>Admin Logins</b> console.</p>
<b>Files (Up/Down)</b>	<p>Displays the number of files uploaded and downloaded. Hover the mouse cursor over the entry in the column for additional information.</p> <p><b>Note:</b> This column is only available in the <b>Cloud Applications</b> console.</p>
<b>FortiASIC</b>	<p>Displays the type of FortiASIC hardware acceleration used in the specified session, if present.</p> <p><b>Note:</b> This column is only available in the <b>All Sessions</b> console, in the <b>now</b> Time Display view.</p>
<b>Group</b>	<p>Displays the group ID associated with the selected session.</p> <p><b>Note:</b> This column is only available in the <b>All Sessions</b> console.</p>
<b>Last Connection Time</b>	<p>Displays the most recent instance of connection to the selected Virtual Private Network (VPN).</p> <p><b>Note:</b> This column is only available in the <b>VPN</b> console.</p>
<b>Level</b> <b>Threat Level</b>	<p>Displays the threat level. Select the column header to sort entries by threat level.</p>
<b>Log ID</b>	<p>Displays the identification number for the data log associated with this entry.</p> <p><b>Note:</b> This column is only available in the <b>All Sessions</b> console.</p>

Column name	Description
<b>Login IDs</b>	<p>Displays the number of login IDs associated with the selected cloud application.</p> <p><b>Note:</b> This column is only available in the <b>Cloud Applications</b> console, in <b>Applications</b> view.</p>
<b>Login Type</b>	<p>Displays the type of login (eg. WEP) associated with the displayed authentication attempt.</p> <p><b>Note:</b> This column is only available in the <b>Failed Authentications</b> console.</p>
<b>Logins</b>	<p>Displays the number of successful logins made by an administrator over the specified time period.</p> <p><b>Note:</b> This column is only available in the <b>Admin Logins</b> console.</p>
<b>Pending</b>	<p><b>Note:</b> This column is only available in the <b>FortiSandbox</b> column, in <b>Source</b> view.</p>
<b>Policy ID</b>	<p>Displays the identification number of the policy under which the selected connection was allowed.</p>
<b>Security Action</b>	<p>Displays the action taken in response to the selected security event. The types of possible actions are as follows:</p> <ul style="list-style-type: none"> <li>• <b>Allowed:</b> No threat was detected and the connection was let through.</li> <li>• <b>Blocked:</b> A threat was detected and the connection was not let through.</li> <li>• <b>Reset:</b> A possible issue was detected and the connection was reset.</li> <li>• <b>Traffic Shape:</b> Some data packets may have been delayed to improve system-wide performance.</li> </ul>
<b>Sessions</b>	<p>Displays the number of sessions associated with the selected destination.</p> <p><b>Note:</b> This column only appears in the <b>Destinations</b> console, in the <b>now</b> Time Display view.</p>
<b>Sessions (Blocked/Allowed)</b>	<p>Displays the number of sessions blocked and allowed by FortiOs.</p> <p>In some consoles, entries can be sorted by number of sessions by selecting the column header..</p>
<b>Severity</b>	<p>Displays the severity level (<b>Critical</b>, <b>High</b>, <b>Medium</b> or <b>Low</b>) associated with the selected security event.</p>

Column name	Description
<b>Source</b>	Displays the source IP address and/or user ID, if applicable.
<b>Source Interface</b>	Displays which interface is being used by the destination server (eg. wan1).
<b>Source Port</b>	Displays the port number being used by the source server to send data.
<b>Source SSID</b>	Displays the Service Set Identifier (SSID) associated with the selected user.  <b>Note:</b> This column is only available in the <b>Wifi Clients</b> console.
<b>Src NAT IP</b> <b>NAT Source</b>	Displays the Network Address Translation (NAT) IP address associated with the source server.
<b>Src NAT Port</b> <b>NAT Source Port</b>	Displays the Network Address Translation (NAT) port number associated with the source server.
<b>Status</b>	The types of possible status' are <b>Malicious</b> , <b>High</b> , <b>Medium</b> , <b>Low</b> , <b>Clean</b> , <b>Unknown</b> , and <b>Pending</b> .  <b>Note:</b> This console is only available in the <b>FortiSandbox</b> console, in <b>Files</b> view.
<b>Submitted</b>	Displays the number of files submitted to the FortiSandbox for assessment in the selected session.  <b>Note:</b> This column is only available in the <b>FortiSandbox</b> console, in <b>Files</b> view.
<b>Threat</b>	Displays the threat type detected in the selected session.
<b>Threat Score (Blocked/Allowed)</b>	Displays the threat score value, a measurement of the total number of threats detected over the course of the session. You can select the column header to sort entries by threat score.
<b>Threat Weight</b>	Displays the threat weight profile associated with the selected session.
<b>Timestamp</b>	Displays the selected session's PHP timestamp.
<b>User</b> <b>User Name</b>	Displays the user name associated with the selected administrator.

---






Column name	Description
<b>Videos Played</b>	Displays the number of videos played via cloud applications.  <b>Note:</b> This column is only available in the <b>Cloud Applications</b> console.



## Risk level indicators

There are currently two consoles within FortiView that display the Risk associated with the console: **Applications** and **Cloud Applications**. Each application pose different levels of risk to the network, represented by a colour code.

The following table identifies each risk level, from least to most severe:

Indicator	Risk	Description
	<b>Green:</b> <i>Risk Level 1</i>	These applications have little to no risk level, with no assigned risk definition. Application file-sharing may result in data leakage, which would be a typical example of a low level risk.  An example application would be the Google toolbar, or Dropbox.
	<b>Blue:</b> <i>Risk Level 2</i>	These applications have an elevated risk level and typically use excessive bandwidth. High bandwidth consumption can lead to increased operational costs.  An example application would be Bittorrent.
	<b>Yellow:</b> <i>Risk Level 3</i>	These applications have a low risk level and are typically evasive.  Evasive applications can lead to compliance risks, and could include applications such as JustinTV and GlypeProxy.
	<b>Orange:</b> <i>Risk Level 4</i>	These applications have a high risk level, and are defined as using both excessive and evasive bandwidth.  Example applications would be AutoHideIP and PandoraTV.
	<b>Red:</b> <i>Risk Level 5</i>	Applications that have a high risk level are prone to malware or vulnerabilities that can introduce business continuity risks.

# Troubleshooting FortiView

## No logging data is displayed

In order for information to appear in the FortiView consoles, disk logging must be selected for the FortiGate unit. To select disk logging, go to **Log & Report > Log Settings**.

Disk logging is disabled by default for some FortiGate units. To enable disk logging, enter the following command in the CLI:

```
config log disk setting
    set status enable
end
```

Only certain FortiGate models support Disk Logging — refer to the [FortiView Feature Support - Platform Matrix on page 9](#) for more information.

## Logging is enabled, but data is not appearing

Some FortiView consoles require certain features to be enabled and working before they will display any data. For example, the Web Filtering FortiView page requires that a Web Filtering profile be configured in **Security Profiles > Web Filter** and then applied to a policy in **Policy & Objects > IPv4 Policy**.

First, ensure the feature is enabled in **System > Feature Visibility**, and then go to the appropriate page to make sure that the feature is being implemented. If it is working but is producing no data, FortiView will have nothing to display.



**FORTINET®**

*High Performance Network Security*



Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.